Assignment 2.2

Cyber Security

Rutwik Ghag

Cyber security grows increasingly important in today’s world, given the availability of information on the internet, and various motives for hacking. Hackers are active for reasons ranging all the way from just experimenting to being cyber terrorists. Hacking is not uncommon anymore as data is extremely valuable today and literally everyone has a need for data. Data is crucial to organizations to extract information to make decisions for the betterment of business.

Automation is an emerging trend in cyber security. The cyber security market is filled with solutions that protect users from potential harmful sources, protect business-critical servers, and protect sensitive data such as personal / private information, healthcare data, intellectual property, and credit card data. Businesses invest in technology to manage these security solutions, often consolidating a vast amount of data into a single system to help organize and access useful information, with the goal of better understanding where they have risk or where certain traffic is coming from or going to. In many cases, the sheer quantity of data to manage is outside the capabilities of the business. That’s where automation comes in. It handles repetitive tasks with ease.

Benefits of Cyber Security Automation:

* Efficient and Cost Effective—Automation allows for faster data collection, making the incident management response a more dynamic, uniform, and efficient process. It also eliminates time-consuming and repeatable tasks, allowing the cyber security experts time to concentrate on creating other strategies and initiatives.
* Fewer Errors—Automation adds artificial intelligence, increasing an organization’s analytic capabilities. It also eliminates the human element from some or all of the process, making a business more efficient and reallocating human resources to where they are most needed.
* Optimize Decision Making—Automated activities will also identify deficiencies that can be corrected through actionable, formalized procedures, leading to a more secure environment.

Since cyber security deals with cyber threats, an important part is dealing with the situation, responding to the incident. In today's day and age of machine learning (ML) and artificial intelligence (AI), the number of organizations leveraging these technological advances to mitigate risk is growing quickly. As fast as the cybersecurity community can develop new solutions predicated on these technologies, malicious actors are developing tools leveraging these technologies as well.

Correlation of data is another new trend in cyber security. Many security vendors collect substantial amounts of threat data. However, data provides little value unless it is organized into actionable next steps. To do this effectively, organizations first need to collect threat data across all attack vectors and from security technologies within their own infrastructure, as well as global threat intelligence outside of their infrastructure. Then, they need to identify groups of threats that behave similarly within the massive amounts of data and use that to predict the attacker’s next step. When using this approach, more data collected results in more accurate results, and reduces the likelihood that the groups identified merely an anomaly. Consequently, the analysis must also have enough computing power to scale today’s threat volume—something that is impossible to do manually. Machine learning and automation allow data sequencing to happen faster, more effectively, and more accurate. Finally, combining this approach with dynamic threat analysis is the only way to accurately detect sophisticated and never-before-seen threats.

Attackers use automation to move fast and deploy new threats at breakneck speeds. The only way to keep up and defend against these threats efficiently is to employ automation as part of your cybersecurity efforts. Hence automation is going to be a crucial part of cyber security from now on, so we might as well embrace it.

[1] <https://www.simplilearn.com/top-cybersecurity-trends-article>

[2] <https://www.forbes.com/sites/forbestechcouncil/2020/11/05/automation-in-the-cybersecurity-world/?sh=4381a4693137>

[3] <https://www.paloaltonetworks.com/cyberpedia/4-ways-cybersecurity-automation-should-be-used>